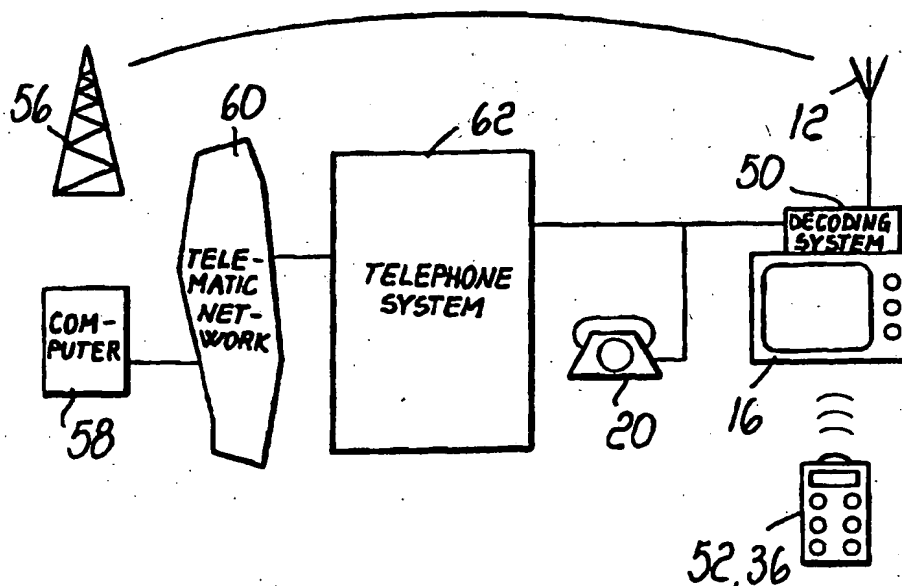




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶: H04N 7/16, 7/173	A1	(11) International Publication Number: WO 95/17796 (43) International Publication Date: 29 June 1995 (29.06.95)
(21) International Application Number: PCT/EP94/04195 (22) International Filing Date: 16 December 1994 (16.12.94) (30) Priority Data: TO93A000967 20 December 1993 (20.12.93) IT (71) Applicant (for all designated States except US): URMET SUD S.P.A. COSTRUZIONI ELETTRICO-TELEFONICHE [IT/IT]; Via di Castel Romano, 167, I-00129 Roma (IT). (72) Inventor; and (75) Inventor/Applicant (for US only): MONDARDINI, Massimo [IT/IT]; Via Mazzini, 40, I-10123 Torino (IT). (74) Agent: MODIANO, Guido; Modiano & Associati, Via Merav- igli, 16, I-20123 Milano (IT).		(81) Designated States: BR, PL, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published With international search report.

(54) Title: SYSTEM FOR ENABLING THE DECODING OF TELEVISION PROGRAMS



(57) Abstract

System for enabling the decoding of television programs comprising a transmitter (36, 52) for wireless signals such as infrared or radio signals, which can be operated by the user with a keyboard; and an overvoice modulator (50) that can be directly connected to a user telephone (20) wire pair which is connected to an overvoice network (62) for connection to a telematic network (60) to which a television station (56, 58) can be connected; said modulator (50) is driven by a transducer that is suitable to receive and convert the signals emitted by the wireless transmitter (36, 52) in order to send, over the telephone wire pair, messages directed to the television station (58). The transmitter (52, 36) is preferably provided in handheld size, is preferably provided with functions for controlling the television set (16), and can be provided with a magnetic card reader.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Larvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

SYSTEM FOR ENABLING THE DECODING OF TELEVISION PROGRAMS

Technical Field

The present invention relates to a system for enabling the decoding of television programs broadcast in encrypted or coded form.

Background Art

Broadcast pay-TV is currently provided mainly by transmitting coded programs and by providing users of the service with a corresponding decoder. The user pays an initial price for the purchase of the decoder and then pays a periodic license or subscription for flat-fee access to all the broadcast programs.

10 It is known that the coding system is essentially an encryption in which one or more of the parameters of the transmitted signal is processed before being broadcast; the decoder performs the reverse process. Coding and decoding are therefore linked to a numeric key which is similar to
15 the encryption keys used in cryptography.

A first drawback of the above described system is that in practice the subscriber pays for the availability the service, not for its actual use: the intensive user pays a low price for each program, whereas the occasional user pays
20 an excessive price that can lead him to renounce the entire service.

Another severe drawback is that the operator of the service must have full control over the sale of decoders, as each sale must be matched by the activation of a
25 subscription contract. This entails maintaining a complex and extensive network for controlling the points of sale.

However, the most severe drawback from the point of

view of the service operator is that the decoders might be duplicated illicitly by external organizations and marketed illegally. The owners of such "pirate" decoders can in fact access the encrypted programs for free and indefinitely
5 without having to pay the corresponding license and without ever being identifiable.

Accordingly, it would be desirable to provide decoded programs to users individually and selectively, that is to say, obtaining from the individual user his approval for
10 viewing the individual program each time, selectively enabling his decoder and charging him the corresponding price.

Disclosure of the Invention

The aim of the invention is therefore to provide a system that allows this selective and individual decoding
15 enabling.

This aim and other objects and advantages which will become apparent from the continuation of the description are achieved by the invention with a system for enabling the decoding of television programs as defined in the appended
20 claims.

Brief description of the drawings

The invention is now described in greater detail with reference to a preferred embodiment, given by way of non-limitative example and shown in the accompanying drawings, wherein:

25 figure 1 is a block diagram of a preferred embodiment of a decoding enabling system according to the invention; and

figure 2 is a block diagram that shows how a system

according to the invention is included operationally in a network for communication with a television station.

Ways of carrying out the invention

It is known that networks for interconnecting user outlets, or wire pairs, connected to the exchanges, and an independent telematic network are among the services currently offered by public telephone systems in some countries. The signals that originate from telephone users and are meant for the telematic network are supplied to the wire pair after being modulated over a carrier frequency outside the voice range, with a method known as "overvoice transmission", so as not to interfere with the normal use of the telephone. This interconnecting network includes exchange equipment located in the exchanges of the public telephone system to receive and demodulate the overvoice messages, decode at least the part of the message that identifies its destination, and then send the message on the external telematic network, where the message is routed to the receiving party. Likewise, the signals transmitted in the opposite direction travel in the same way.

An interconnecting network such as the one described above has been installed for example in Italy by Telecom and is known as "Argotel".

According to the present invention, the decoder associated with the television set of the user to decode the encrypted television signal is provided with an overvoice modem which is connected to the "Argotel" telematic network by means of the home telephone wire pair of the user, so as to receive an enabling signal from a television station which is connected to said telematic network. The user,

again by means of the overvoice modem, can send to the television station a signal that approves the enabling of the decoder and thus the charging of the service to his account. Enabling furthermore occurs preferably by sending
5 an approval key which is specific for the individual user and is linked to a code that is hardwired into his decoder, as explained hereinafter. This obviously makes it impossible to use illegal decoders, since the enabling signal sent by the exchange is a function of the code that is hardwired or
10 stored in the decoder and varies with each individual user.

In figure 1, a decoder 10 is connected to an antenna 12 so that it can receive an encrypted television signal, decode it by using a decoding key CHD received at an input 14, and apply the decoded television signal to a television
15 set 16.

A user telephone wire pair 18 is furthermore connected to a telephone exchange, not shown, and through said exchange also to an "Argotel" telematic network, which is also not shown. The telephone wire pair 18 is connected not
20 only to the conventional telephone set 20 but also to an overvoice modem 22 which is also known as overvoice terminal (TOV) and is per se known. The TOV has an output 24 on which it can output a signal that arrives from the telematic network and consists of a decoding enabling code AD; the TOV
25 22 also has an input 26 on which it can receive a signal that consists of a user identification code IU to transmit it to the telematic network as part of a message to be sent to a television station according to a preset protocol which is not part of the present invention. Said user
30 identification code IU is contained in a ROM 30 and can be

transferred to the input 26 of the TOV 22 by means of a port 32 that can be enabled by an infrared-ray sensor 34 when it receives an approval signal from an infrared-ray remote control 36 which can in turn be operated by the user by means of a keyboard. The remote control 36 is preferably produced in portable form, so that it can be easily be held in the hand by the viewer during use (so-called handheld format) and can be integrated with the conventional remote control of the television set 16.

10 The output 24 of the TOV 22 on which the enabling code AD is output is connected to a first input of a combiner circuit 38 which has a second input that receives a personal user code PU from a ROM 40. The combiner circuit 38 is configured so as to combine the enabling code AD received from the TOV with the personal user code PU according to a preset arbitrary algorithm, so as to provide, on an output 41, a decoding key CHD which is applied to the decoder 10.

The operation of the decoding system shown in figure 1 is now described with reference to figure 2.

20 In figure 2, the decoding system which is surrounded by a dashed line in figure 1 is generally designated by the reference numeral 50 and is connected to the television set 16, with which a remote control 52 is associated; said remote control also includes the functions of the remote control 36 of figure 1. The system receives, by means of the receiving antenna 12, a television program transmitted by a television camera, not shown, by means of a broadcasting antenna 56. The television station furthermore has a computer 58 which is connected to a telematic network, for example the "Argotel" packet-switching network,

30

schematically designated by the reference numeral 60. The "Argotel" network is linked to the telephone system 62 in a per se known manner.

Before the encrypted program begins, the television station broadcasts on television an uncoded message regarding the program about to be broadcast, inviting viewers to accept it, that it so say, signal their approval for purchase. If the user accepts, he operates the remote control 36 to energize the sensor 34 and enable the transfer of his identification code IU from the ROM 30 to the TOV 22 and thus to the telephone wire pair, as part of an overall message, based on a known protocol, that finally reaches, over the telematic network 60, the computer 58 of the television station. The computer records the message, checks the user's credit by charging the service to his account, and finally sends over the telematic network 60 a reply message which is addressed to the user and contains an enabling code AD that is specific for that user. The TOV 22 receives the message and outputs the enabling code AD on its output 24, and therefore on the first input of the combiner circuit 38, which combines said code with the personal user code PU supplied by the ROM 40, according to a preset algorithm. The enabling code AD is chosen by the station so that the decoding key CHD used by the decoder 10 to decode is generated when the enabling code AD is combined with the personal user code PU according to the selected algorithm.

The ROMs 30 and 40, which are shown separately in figure 1, are in practice a single data memory, for example in the form of an integrated circuit which is enclosed in a cartridge or card that can be inserted in a connector of the

apparatus, and is delivered to the user when he approves the subscription contract. As an alternative, the apparatus may be provided with a reader for cards with magnetic bands and the codes can be recorded on a corresponding card. Or, also, 5 the codes can be written in the integrated circuit of a chip-card. In the case of the magnetic-band card or of the chip-card, said cards can also act as credit cards and also include data related to the user's credit.

It is evident to the expert in the field that the 10 structure and operating method of packet-based telematic networks, and particularly of the "Argotel" network, allow to deal with considerable peaks of demand without overloading. In other words, these networks are well-suited for meeting requests for the purchase of television 15 programs, which are necessarily concentrated in short periods shortly before the individual programs, especially those most appreciated by viewers.

The invention offers several advantages with respect to known forms of encrypted pay-TV, including:

20 a) the viewer only pays the charge for the desired programs, and the annual cost of the service for that viewer is proportional to actual use;

b) it is no longer necessary to keep control over decoder sales, which can indeed be fully liberalized; when 25 he registers as a subscriber at the television station, the user receives a card or cartridge which contains his personal codes as described above and must be inserted in the decoder;

c) the possibilities of fraud are substantially 30 eliminated: even if a fraudulent user managed, by chance or

by spying, to learn the decoding key in a given case, with the system according to the invention the key can be changed at any time, from one program to the next, or even during the same program.

5 A preferred embodiment in a simplified form has been described and can be modified and changed in many ways by using means that are known to the expert. For example, the television station might send a single enabling message that includes a validity period or send two messages in sequence,
10 one for enabling decoded viewing on the part of the user and one for disabling it. Purchase approval might furthermore be given not by a remote control, but with a button on the decoder cabinet, optionally protected by a key or controlled with a credit card. The encoding or encryption methods may
15 also be any of the several known ones in which the algorithm includes a decoding key. It is also evident that the teachings of the invention can also be applied by transmitting the user approval messages and the decoding enabling messages from the television station over the
20 conventional dial-up telephone network instead of at overvoice frequencies: this solution might be preferable in particular cases. In general, the operating methods may be developed or improved on the basis of the described principle.

CLAIMS

1 1. System for enabling the decoding, at a user's
2 location, of television programs broadcast by a station,
3 characterized in that it comprises:

4 - a decoder (10) which is adapted to receive a coded
5 television signal and to decode it by processing based on a
6 digital decoding key (CHD) which can be applied to one of
7 its inputs;

8 - an overvoice modem (22) which can be directly
9 connected to a user telephone wire pair which is connected
10 to an overvoice network (62) for connection to a telematic
11 network (60) to which a computer (58) of the television
12 station can be connected;

13 - permanent memory means (30, 40) for storing at least
14 one user identification code (IU) and a personal user code
15 (PU);

16 - control means (32) for activating said modem so that
17 it sends a message in overvoice, said message being directed
18 to said computer (58) of the television station and
19 containing said user identification code, in order to cause
20 said computer (58) to send an overvoice message which is
21 directed to said overvoice terminal (22) and contains a
22 decoding enabling code (AD); and

23 - a combiner circuit (38) for combining, according to a
24 preset algorithm, the personal user code (PU) with said
25 decoding enabling code (AD) obtained from said user
26 terminal.

1 2. Decoding enabling system according to claim 1,
2 characterized in that said control means are constituted by

3 a port (32) between said permanent memory means (30) and an
4 activation input (26) of said modem (22) and in that said
5 port (32) can be activated by the user.

1 3. Decoding enabling system according to claim 2,
2 characterized in that said port (32) can be activated by an
3 infrared-ray remote control (36) which is suitable to
4 activate an infrared-ray sensor (34) connected to a port
5 enabling input.

1 4. Decoding enabling system according to claim 3,
2 characterized in that said remote control (36) is provided
3 in handheld size.

1 5. Decoding enabling system according to claim 3 or 4,
2 characterized in that said remote control (36) is integrated
3 in a remote control (52) for activating the functions of a
4 television set.

1 6. Decoding enabling system according to one of claims
2 1 to 5, characterized in that said permanent memory means,
3 (30,40) are constituted by a ROM.

1 7. Decoding enabling system according to one of claims
2 1 to 5, characterized in that said permanent memory means
3 (30,40) are constituted by a magnetic card or by a chip-
4 card.

1 8. Decoding enabling system according to one of claims
2 1 to 7, characterized in that said control means (32)
3 comprise a magnetic card or chip-card reader.

1 / 1

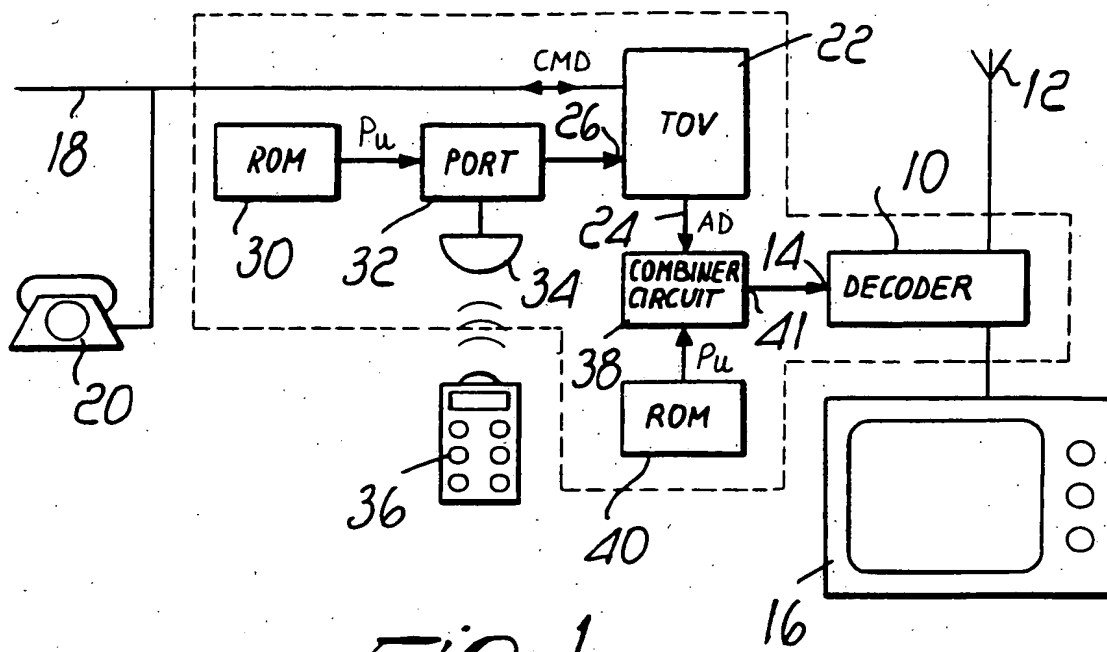


Fig. 1

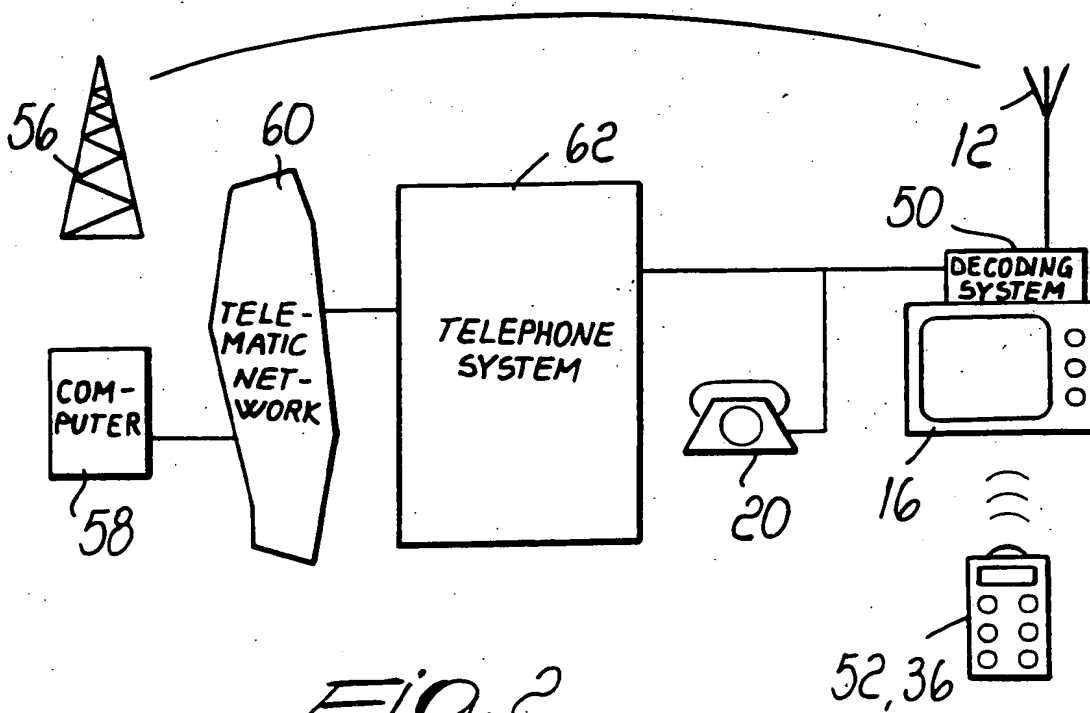


Fig. 2

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 94/04195

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 6 H04N7/16 H04N7/173

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A,5 270 809 (GAMMIE ET AL.) 14 December 1993	1
A	see column 1, line 37 - column 2, line 25 see column 5, line 63 - column 6, line 44	2-8
Y	SYMPOSIUM RECORD - CATV SESSIONS, 14 June 1991, MONTREUX, SWITZERLAND pages 229 - 238 REMME 'DATA OVER TELEPHONY/TV-EXCHANGE' see the whole document	1
A	EP,A,0 489 385 (TECNOENERGIA BY TEL) 10 June 1992 see the whole document	1-8
A	EP,A,0 506 435 (SCIENTIFIC-ATLANTA) 30 September 1992 see page 10, line 45 - page 11, line 25	1-8
	--- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

3 March 1995

Date of mailing of the international search report

06.04.95

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax (+31-70) 340-3016

Authorized officer

Greve, M

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/EP 94/04195

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 542 047 (TELENORMA) 19 May 1993 see abstract -----	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 94/04195

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5270809	14-12-93	AU-B- 647255 AU-A- 1383892	17-03-94 08-10-92
EP-A-0489385	10-06-92	NONE	
EP-A-0506435	30-09-92	US-A- 5237610 AU-B- 650958 AU-A- 1384092 CN-A- 1066950 JP-A- 5145923	17-08-93 07-07-94 01-10-92 09-12-92 11-06-93
EP-A-0542047	19-05-93	DE-A- 4217649 EP-A- 0542048	02-12-93 19-05-93